The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
08/12/2020

SUBJECT:
A Vulnerability in Zoho ManageEngine ADSelfService Plus Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in Zoho ManageEngine ADSelfService Plus, which could allow for remote code execution. ManageEngine ADSelfService Plus is an integrated Active Directory self-service password management and single sign on solution by ZOHO Corporation. Successful exploitation of this vulnerability may allow an unauthenticated attacker to remotely execute commands with system level privileges on target windows host. An attacker can exploit this issue to execute arbitrary code in the context of the affected system. Failed exploit attempts may result in a denial-of-service condition.

THREAT INTELLIGENCE:
A proof of concept for this vulnerability has been made available on YouTube.

SYSTEMS AFFECTED:
- Zoho ManageEngine ADSelfService Plus prior to 6.0 Build 6003 are vulnerable

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in Zoho ManageEngine ADSelfService Plus, which could allow for remote code execution. ManageEngine ADSelfService Plus is an integrated Active Directory self-service password management and single sign on solution by ZOHO Corporation. This vulnerability exists within the self-service option on the Windows login screen. Upon selecting this option, the thick-client software is launched, which connects to a remote

ADSelfService Plus server to facilitate self-service operations. An unauthenticated attacker having physical access to the host could trigger a security alert by supplying a self-signed SSL certificate to the client. The View Certificate option from the security alert allows an attacker to export a displayed certificate to a file. This can further cascade to a dialog that can open Explorer as SYSTEM. By navigating from Explorer to \windows\system32, cmd.exe can be launched as a SYSTEM.

RECOMMENDATIONS:
The following actions should be taken:

- Apply the stable channel update provided by ZOHO Corporation to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Patch Update:
https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6003-release-faceid-support

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11552

Disclosure:
https://seclists.org/fulldisclosure/2020/Aug/4

Proof of Concept:
https://www.youtube.com/watch?v=slZRXffswnQ